PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-347946

(43)Date of publication of application : 15.12.2000

(51)Int.Cl. G06F 12/14
G06F 15/00

(21)Application number : 2000-112562

(22)Date of filing : 13.04.2000

(71)Applicant : DEUTSCHE THOMSON BRANDT GMBH

(72)Inventor : HERPEL CARSTEN
SCHREIBER ULRICH
AUST ANDREAS
BOEHM JOHANNES

(30)Priority

Priority number	Priority date	Priority country
99 99107643	16.04.1999	EP
99 99108640	12.05.1999	EP

(54) METHOD AND DEVICE FOR PREVENTING ILLEGAL USE OF MULTIMEDIA CONTENTS

(57)Abstract:

PROBLEM TO BE SOLVED: To prevent the illegal use of multimedia contents by enciphering the contents and transferring data related to usage from a storage device to the other storage device by transmitting a cryptographic key from a contents subscriber.

SOLUTION: Concerning a procedure for transferring a multimedia contents item and the usage, which is embedded in the contents subscriber, related to that contents item from the first storage device to the second storage device, first of all, when the multimedia contents item does not exist in the second device yet, copying to the second device is performed. Secondly, the contents subscriber is copied to the second storage device. In the case of enciphered or partially enciphered contents, this subscriber has a decipher key effective for the first device. Thirdly, the contents in the first storage device are removed. Fourthly, a new decipher key is generated for using the contents item in the second storage device and inserted into the copied contents subscriber.

LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁　(JP)

(12) 公開特許公報（Ａ）

(11) 特許出願公開番号

特開２０００－３４７９４６

（Ｐ２０００－３４７９４６Ａ）

(43) 公開日　平成12年12月15日(2000.12.15)

(51)Int.Cl.[7]		識別記号	F I			テーマコード(参考)
Ｇ０６Ｆ	12/14	３２０	Ｇ０６Ｆ	12/14	３２０　Ｅ	
	15/00	３３０		15/00	３３０　Ｚ	

審査請求　未請求　請求項の数　１５　ＯＬ　（全５頁）

(21) 出願番号　特願2000-112562(P2000-112562)

(22) 出願日　平成12年4月13日(2000.4.13)

(31) 優先権主張番号　99107643:1

(32) 優先日　平成11年4月16日(1999.4.16)

(33) 優先権主張国　欧州特許庁（ＥＰ）

(31) 優先権主張番号　99108640:6

(32) 優先日　平成11年5月12日(1999.5.12)

(33) 優先権主張国　欧州特許庁（ＥＰ）

(71) 出願人　595033034
ドイチェ　トムソンーブラント　ゲーエム　ベーハー
Ｄｅｕｔｓｃｈｅ　Ｔｈｏｍｓｏｎ－Ｂｒａｎｄｔ　ＧｍｂＨ
ドイツ連邦共和国　デーー78048　ヴィリンゲンーシュヴェニンゲン　ヘルマンーシュヴェーアーシュトラーセ　3

(72) 発明者　カーステン　ヘルペル
ドイツ連邦共和国，30171　ハノーヴァー，グローセ・バーリンゲ　61

(74) 代理人　100070150
弁理士　伊東　忠彦　（外1名）

最終頁に続く

(54)【発明の名称】マルチメディアコンテンツの不正な使用を防止する方法及び装置

(57)【要約】　（修正有）

【課題】　コンテンツの著者又は権利の所有者と正当なユーザとの両方が満足するために、正当なマルチメディアコンテンツ項目に関連する権利を管理する方法を提供する。

【解決手段】　メディアサーバとして使用され得る大容量記憶装置では、コンテンツを移動する簡単な方法及び使用権を必要とする。権利を新しい位置へ移動することは、その新しい位置での項目が正当な原本であることを意味する。これは項目の前の原本と新しいバーションとの間で原本又は複製物かを示すフラグの値を交換することで達成され得る。暗号化されたコンテンツを含むデジタルシステムでは、マルチメディアコンテンツ項目に関連する権利を説明する記述子及び関連する位置特定復号化鍵によっても達成され得る。マルチメディアコンテンツ項目の原本は第１の大容量記憶装置、又はメディアサーバから削除される必要は無く、第２の記憶装置に再生権を一時的に渡す。

【特許請求の範囲】

【請求項１】　第１の大容量記憶装置に記憶されるマルチメディアコンテンツの不正な使用を防止する方法であって、

上記マルチメディアコンテンツは暗号化され、又は部分的に暗号化され、

上記マルチメディアコンテンツはコンテンツ記述子ではっきりとラベル付けされ、

上記コンテンツ記述子は上記マルチメディアコンテンツ項目に関連する権利を伝達し、

上記コンテンツ記述子は、上記マルチメディアコンテンツ項目に関連する暗号鍵を伝達し、

各上記マルチメディアコンテンツ項目の使用権に関するデータは、上記第１の記憶装置から上記マルチメディアコンテンツを削除すること無く上記マルチメディアコンテンツ項目及び上記コンテンツ記述子の両方を伝送することによって、上記第１の記憶装置から第２の記憶装置へ移動されることを特徴とする方法。

【請求項２】　上記マルチメディアコンテンツ項目が既に上記第２の記憶装置に存在する場合、上記コンテンツ記述子のみが上記第１の記憶装置から上記第２の記憶装置へ伝送される請求項１記載の方法。

【請求項３】　コンテンツ記述子によるマルチメディアコンテンツ項目のはっきりとしたラベル付けは、上記マルチメディアコンテンツ項目に挿入されると共に上記コンテンツ記述子の一部として伝達される補助的な認可信号によって達成される請求項１記載の方法。

【請求項４】　上記暗号鍵はマルチメディアコンテンツ項目をマルチメディア再生アプリケーションの特定なインスタンスに関して所与の記憶位置のみで使用することを可能にする請求項１記載の方法。

【請求項５】　マルチメディアコンテンツ項目に関連する権利に関するデータを上記第１の記憶装置から上記第２の記憶装置へ移動することは、確実な通信チャネルを通じて信頼度が高いソフトウェア又は専用のハードウェアを使用することで成される請求項１又は２記載の方法。

【請求項６】　上記マルチメディアコンテンツ項目を選択的にコピーした後、第１に、上記コンテンツ記述子が上記第２の記憶装置にコピーされ、第２に、マルチメディアコンテンツの原本のための上記復号鍵を含む上記コンテンツ記述子が上記第１の記憶装置から削除され、第３に、第２の記憶装置で上記マルチメディアコンテンツ項目の使用のための新しい復号鍵が発生されて上記コピーされたコンテンツ記述子の中に挿入される、請求項１又は２記載の方法。

【請求項７】　追加的な復号鍵は上記第１の記憶装置のために許可の下で発生される請求項６記載の方法。

【請求項８】　上記コンテンツ記述子の中の権利証明書は、上記マルチメディアコンテンツの原本が非制限的な権利を有し、複製物が制限された権利を有するとして特定する原本／複製物標識によって実施される、請求項１記載の方法。

【請求項９】　原本／複製物標識でラベル付けされたマルチメディアコンテンツの項目の原本を第１の記憶装置から第２の記憶装置へ移動する段階を含む方法であり、

原本／複製物標識が複製物であることを示すようセットされた項目をコピーする段階と、

上記原本ファイルの中の原本／複製物標識をコピー状態にリセットする段階と、

新しいファイルの中の原本／複製物標識が原本であることを示すようセットする段階とを有する、請求項１乃至８のうちいずれか一項記載の方法。

【請求項１０】　検証処理が起動され、上記マルチメディアコンテンツ項目を上記第１の記憶装置から上記第２の記憶装置へ移動することに成功すれば、上記第１の記憶装置にあるマルチメディアコンテンツ項目の前の原本は削除される請求項１乃至９のうちいずれか一項記載の方法。

【請求項１１】　上記マルチメディアコンテンツ項目を移動することが許される場合、上記第１の記憶装置及び上記第２の記憶装置のユーザインターフェイスの中の移動表示器が有効とされる、請求項１乃至１０のうちいずれか一項記載の方法。

【請求項１２】　上記コンテンツ記述子は源又は受信装置の移動可能でない記憶域内に記憶される請求項１記載の方法。

【請求項１３】　上記コンテンツ記述子は、

復号化のための鍵と、

暗号化されたマルチメディアコンテンツ項目の部分及び暗号化スキームを表示する暗号化記述子と、

上記マルチメディアコンテンツ項目が原本か複製物かを示すフラグと、

コピー状態及びコピー生成回数カウンタと表示するコピー記述子と、

上記マルチメディアコンテンツ項目が源又は受信装置によって使用可能であることを表示するマルチメディアコンテンツ項目アクティブ記述子とのうちの一つ以上を含む、請求項１記載の方法。

【請求項１４】　上記信頼度が高いソフトウェア又は専用のハードウェアは、マルチメディアコンテンツ項目に関連する権利に関わるデータを確実な通信チャネルを通じて第３者に移動する処理のための権限を選択的に得る、請求項１乃至５記載のうちいずれか一項記載の方法。

【請求項１５】　第１の記憶装置に記憶されマルチメディアコンテンツの不正な使用を防止する装置であって、

上記マルチメディアコンテンツを暗号化し、又は部分的に暗号化する手段と、

上記マルチメディアコンテンツに関連する権利及び／又

は暗号鍵を伝達するコンテンツ記述子によって上記マルチメディアコンテンツをはっきりとラベル付けする手段と、

上記第１の記憶装置から上記マルチメディアコンテンツを削除すること無く上記マルチメディアコンテンツ項目及び上記コンテンツ記述子の両方を伝送することによって、各上記マルチメディアコンテンツ項目の使用権に関するデータを上記第１の記憶装置から第２の記憶装置へ移動する手段を特徴とする装置。

【発明の詳細な説明】

【０００１】

【発明が属する技術分野】本発明は、マルチメディアコンテンツを不正にコピーすることを防止する一方でコンテンツの正当なユーザのために十分な柔軟性を保持する方法に関する。

【０００２】

【従来の技術】ＤＡＴ及びＭｉｎｉＤｉｓｋのような現在のデジタル媒体は、コンテンツ項目のデジタル複製物を複数生成することを防止する機構を有する。その場合、一つのデジタル複製物のみが認可される。将来的なデジタルマルチメディアシステムによって、コピーの保護はより洗練され、且つ、より一層実行可能となる。

【０００３】この将来的なマルチメディアシステムは、コンテンツ項目を異なる記憶媒体間（即ちディスク、テープ）で自由に移動することを「コピー」されていると認識するため、正当なユーザはコンテンツを異なる記憶媒体間で自由に移動し得ないといった不利な点を有し得る。このため、更なるコピー動作は不正となり装置によって禁止される。

【０００４】デジタルマルチメディア源からの複製物がデジタルではなくアナログ領域で生成される場合、コピー動作は現在の既存のデジタルオーディオ又はビデオによって制限されないが、複製物の品質は劣る。

【０００５】さもなければ、ＭＰ３フォーマットでデジタルに暗号化された音楽のようなデジタルマルチメディアコンテンツは現在でも、インターネットからの購読でダウンロードされ得、その後品質が劣ること無く、又、追加費用をコンテンツの所有者に支払うこと無く自由にコピーされ得る。

【０００６】

【発明が解決しようとする課題】本発明は、マルチメディアコンテンツの不正な使用を防止する一方で、コンテンツの正当なユーザのために十分な柔軟性を保持する新しい方法と、このような方法を実行する装置を開示することを目的とする。

【０００７】

【課題を解決するための手段】本発明によると、上記目的は主クレームで記載される特徴を含む手段によって達成される。有利な設計及び発展は従属項で記載される。

【０００８】デジタル音楽、ビデオ又はソフトウェアの

ようなデジタルマルチメディアコンテンツの配布フォーマットの広がりによって、マルチメディアコンテンツ項目の認可されないコピー動作は、コンテンツの著者又は権利の所有者の観点からするとより一層問題となる。しかしながら、コンテンツへのアクセス可能性における制限は必要であるが、この制限は権利の正当な所有者がこのコンテンツ項目を使用する上で妨害になってはならない。

【０００９】マルチメディアコンテンツは、将来的に家庭用娯楽機器の一つとなる大容量記憶装置、又はメディアサーバに記憶されることが予想される。他方で、再生に使用されるモバイル装置（移動式装置）がある。各マルチメディアコンテンツに関連するコンテンツ記述子は、コンテンツの使用における全ての制限が維持されることを保証しつつ、ユーザの観点による柔軟な方法でコンテンツの使用を管理するための基礎となる。特に、本発明で詳述されるようにこのようなコンテンツ記述子は完全なマルチメディアコンテンツ項目を移動する代わりにコンテンツ項目の使用権のみを一方の装置から他方の装置へ移動することを可能にすることで、コンテンツ項目自体の不必要なコピー動作を回避することが出来る。権利を移動することは、新しい位置におけるマルチメディアコンテンツ項目が再生され得る正当な原本となり、且つ、関連する権利によって許可されればその新しい位置におけるマルチメディアコンテンツ項目から例えば一つの更なる複製物が生成され得ることを意味する。

【００１０】簡単な実施例では、権利の移動は項目の前の原本と新しいバージョンとの間で原本又は複製物かを示すフラグの値を交換することで達成され得る。暗号化された又は部分的に暗号化されたコンテンツを含む将来的なデジタルシステムは、マルチメディアコンテンツ項目に関連する権利を記述し、又、位置特定復号鍵を含む上記コンテンツ記述子によって達成され得る。有利には、マルチメディアコンテンツ項目の原本は第１の大容量記憶装置又はメディアサーバから削除される必要は無く、できればモバイル装置である第２の記憶装置に再生権を一時的に渡すことを可能にする。

【００１１】オーディオ、ビデオ、テキスト、ゲーム、ソフトウェア等のようなデジタルマルチメディア素材は、消費者電子機器及びコンピュータプラットフォームの両方で利用可能となる。本発明は、マルチメディアコンテンツ項目の位置とは無関係なものとする。このことは、このような状況で実際により重要となる。

【００１２】

【発明の実施の形態】本発明の実施例は以下の説明でより詳細に説明する。

【００１３】本発明は、コンテンツ項目に関連する正当な権利を特定するコンテンツ記述子を伴うマルチメディアコンテンツ項目を提供する。コンテンツ記述子は、そのコンテンツ項目に関するオブジェクト又はストリーム

識別子を参照することでマルチメディアコンテンツに関連され得る。このような関連性を明白にし、又、それが容易に破られ得ないことを確実にするために、コンテンツ項目のための特殊な署名が電子透かしのような手段でコンテンツ信号自体に含まれ得る。同じ署名がこのときコンテンツ記述子に参照され得る。コンテンツ記述子はユーザに可視でないと考えられ、認証の手段を用いることにより、改竄される心配がなくされる。

【００１４】使用権の情報を伝達するコンテンツ記述子とコンテンツ自体との間のこのような確実な繋がりは、本願の請求項に記載されるように実際のマルチメディアコンテンツを自由にコピーする一方でそれを使用する能力に対する強い制御を維持するための手順を確立することを可能にする。これは、例えばユーザの自宅にあるメディアサーバと携帯用再生装置との間のように異なる記憶装置と再生装置との間でコンテンツ項目が頻繁に交換されるとき、特に重要となる。携帯用装置の記憶容量によって、頻繁に再生されるコンテンツは毎回メディアサーバからコピーされる必要はない。項目が携帯用装置に物理的にまだ存在する限り、比較的少ない量のデータである使用ライセンスのみがメディアサーバと携帯用装置との間で交換されるべきである。それ故に、限られた数の同時に存在する複製物にのみ認可されるコンテンツは複数の装置に効率的に使用され得る。

【００１５】マルチメディアコンテンツ項目及びコンテンツ記述子に埋め込まれたそのコンテンツ項目に関する使用権を第１の記憶装置からできれば再生装置である第２の記憶装置に転送する手順は、改竄される心配があってはならない。以下の段階、即ち第１に、マルチメディアコンテンツ項目自体がまだ第２の装置に存在しない場合は第２の装置にコピーされる段階が続くべきである。更に、第２に、コンテンツ記述子が第２の記憶装置にコピーされる。暗号化された若しくは部分的に暗号化されたコンテンツの場合、この記述子は第１の装置に有効な復号鍵を有する。第３に、第１の記憶装置のコンテンツ記述子が除去される。更に、第４の段階として第２の記憶装置におけるマルチメディアコンテンツ項目の使用のために新しい復号鍵が発生されコピーされたコンテンツ記述子の中に挿入される。

【００１６】上記手順は、有利に、復号鍵が単一の記憶装置又は単一の再生アプリケーションのためのみに有効であるとする。このため、コピーされたコンテンツ記述子を含むコピーされたマルチメディアコンテンツ項目は、新しい鍵が発生されるまでは第２の記憶装置で再生可能でない。この場合、手順を中断することによって、ライセンスの不法な重複に関して改竄される心配がない。

【００１７】有利にこの手順は、信用度が高いソフトウェア又は専用のハードウェアによって取扱われる。この手順の安全性を更に改善するためには、特に処理がインターネットのような広域ネットワークで行なわれる場合、装置間で安全な通信チャネルが使用されるべきである。選択肢として、信用度が高いソフトウェア又は専用のハードウェアも、上記手順を認可する第３者への安全な通信チャネルを確立し得る。この手順後、マルチメディアコンテンツ項目は第１及び第２の記憶装置の両方の装置に物理的に存在する。しかしながら、このコンテンツ項目はコンテンツ記述子の形態でのライセンスが第１の記憶装置に戻されるまで、第２の記憶装置のみで再生可能である。

【００１８】選択肢として、課される費用の支払後、第２の記憶装置に転送されるライセンスとは無関係に第１の記憶装置のコンテンツをアクセス可能にするために、追加的ライセンスが発生され得る。反対に、マルチメディアコンテンツ項目がもはや第１の記憶装置で必要でなくなると、そのとき第２の記憶装置が項目の原本に元々関連する権利を全て含む複製物を有するため、第１の記憶装置のマルチメディアコンテンツ項目は物理的に削除され得る。具体的には、このコンテンツ項目は使用権及び更なる第３の記憶装置にマルチメディアコンテンツ項目をいつでも移動する権利を含む。使用権はマルチメディアコンテンツ項目の複製物を一つ以上生成するための許可を含む。

【００１９】メディアサーバが常にマルチメディアコンテンツ項目の完全なデータベースを維持することが好ましい。このデータからの認証される再生可能な複製物の数は、前述の手順で制御され得る。複製物が生成される度、サーバのライセンスデータベースは適当に更新される。ライセンス情報の状態に依存して、更なる複製物を生成することは可能でなくなり得る。

【００２０】更なる好ましい実施例では、コンテンツ記述子は原本／複製物フラグを含む幾つかのフラグを有する。原本に関連する権利は、コンテンツ項目のデジタル複製物を一つ生成することを許可することを含む一方で、既に複製物とマーク付けされているコンテンツ項目から更なる複製物は生成され得ない。

【００２１】この場合、マルチメディアコンテンツ項目の権利を移動することは以下の手順に対応する。第１に、原本／複製物フラグが「コピー」であることを示すようセットされたマルチメディアコンテンツ項目をコピーする段階を有する。更に、原本ファイルの原本／複製物フラグを「コピー」状態にリセットし、新しいファイルの原本／複製物フラグを「原本」であることを示すようセットする段階を有する。これは、電力異常等の場合、最悪の場合では項目の両方のバージョンが複製物であるとラベル付けされるため改竄される心配がない。選択肢として、検証処理が起動され得、最終的な段階として原本項目は複製物として保持されていなければその原本の項目は削除され得る。

【００２２】更なる好ましい実施例では、この手順はマ

7

ルチメディアコンテンツのみではなくマルチメディアプレイヤー、辞書、ルートプランナーのようなソフトウェアアプリケーション自体にも適用し得る。

【００２３】マルチメディアコンテンツ項目のためのコンテンツ記述子は、・復号のための鍵と、メディアファイルで暗号化された部分及び暗号スキームを表示する暗

8

＊号記述子と、ファイルが原本か若しくは複製物かを示すフラグ（原本／複製物フラグ）と、コピー状態を表示するコピービット、例えばＣＧＭＳビット及びコピー生成回数カウンタと、メディアファイルが装置によって使用可能かを表示するメディアアクティブビットとのうちのいずれかの要素を少なくとも一つ含む。

フロントページの続き

(72)発明者　ウルリヒ　シュライバー
ドイツ連邦共和国，30827　ガルブセン，
ライフアインゼンシュトラーセ　7

(72)発明者　アンドレーアス　アオスト
ドイツ連邦共和国，30177　ハノーヴァー，
シュトルムシュトラーセ　23

(72)発明者　ヨハネス　ベーム
ドイツ連邦共和国，37083　ゲッティンゲン，アカーツィエンヴェーク　54